Threat / Hazard Rating Definitions (DRAFT) – The following baseline definitions of threat and hazard can serve as a starting basis for discussion within both the USMC MA community, and the DOD Intel Community (such as DIA). There are significant differences from the DOD ETHA draft requirements and focus.

Critical (.76 -1.00)-- Indicates an imminent threat against the asset or the immediate area where the asset is located.

- For man-made threats (criminal, terrorist, insider, etc) the threat has both the capability and intent to cause a disruption and the Asset or similar assets are being targeted on a frequent or recurring basis.
- For naturally occurring events (flood, tornado, hurricane, earthquake, etc.), or accidental disruption (construction mishap, accident, design flaw, etc.), the hazard has a significant capability to cause a disruption and a demonstrated history of occurring on a very frequent basis.

High (.51 to .75) - Indicates a credible threat against the asset or the immediate area where the asset is located.

- For man-made threats, this is based on the knowledge of the threat's capability, the intent to cause disruption to the asset based on related incidents that took place at similar assets or locations, and a demonstrated history of occurrence.
- For naturally occurring hazards and accidental disruptions, the hazard has a significant capability to cause damage to the asset with a demonstrated history of occurring on an occasional basis , which may change under specified conditions.

Medium (.26 to .50)-- Indicates a potential threat to the asset or the immediate area where the asset is located.

- For man-made threats, it is based on the threats intent to compromise the asset and the possibility that the threat could obtain the capability through alternate sources where the capability has been demonstrated in related incidents.
- Also indicates there is a significant capability with low or no current intent, which may change under specified conditions, and low or no demonstrated history.
- For naturally occurring hazards and accidental disruptions, it is based on the hazard's significant capability to cause damage to the asset with a demonstrated history of occurring on an infrequent basis which may change under specified conditions.

Low (.01- .25) -- Indicates little or no credible evidence of a threat to the asset or the immediate area where the asset is located.

- For man-made threats, it is based on little or no credible evidence of capability or intent with no demonstrated history of occurrence against the asset or similar assets.
- For naturally occurring hazards and accidental disruptions, it is based on little or no credible evidence of the capability to cause damage to the asset, which may change under specified conditions, and there is no history of occurrence.

Risk Assessment Methodology. All mission assurance elements will utilize the USMC Asset Priority Methodology (USMC-APM) System to standardize the critical asset prioritization/criticality in conjunction with the USMC Risk Assessment (USMC-RA) Tool to obtain an objective risk rating. MC-CAMS Next Generation can also be used to calculate critical asset risk rating, because USMC-APM and the USMC-RA tool are

(1) incorporated within the system. Use of MC-CAMS Next Generation ensures risk management will be executed uniformly across all elements of MA.

(2) Updating Critical Asset Risk Profile/Rating. Critical asset risk profiles/ratings will be updated annually or when changes in the criticality, threats/hazards, or vulnerability occur. Significant increases in risk profiles/ratings may require changes in mitigation/remediation strategies and resource generation priorities.

3003. Risk Analysis. Risk Response. While the risk assessment process seeks to evaluate and identify risk of loss to assets based on an asset's criticality (mission impact), the likelihood of threats and hazards occurring, and associated degrees of vulnerabilities, risk response is the process of determining options and actions to reduce the risk of loss to the asset, and thus reduce impact on mission execution. The options/action steps include remediation of risk, mitigating the effects of loss once threat/hazard event occurs, reconstituting the asset's capabilities after loss or disruption, acknowledging the risk, or simply transferring the risk decision to a higher echelon of command. To complete risk response planning, commands can use selected members from the the MA Working Group, or commands may establish a remediation/mitigation team consisting of experienced personnel with necessary expertise for developing risk response plans. The following discusses each risk response option/action in further detail.

a. Remediation. Remediation is defined as actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified. Remediation involves identifying countermeasures that can be implemented before undesirable events or attacks occur that could exploit the identified vulnerabilities. MA planners will prioritize their remediation efforts on those assets with highest impact to supported missions if those assets were lost; address the threats and hazards that have the highest rated probability of occurrence; and address the most significant asset vulnerabilities identified that could be exploited by the most likely threats or hazards. To ensure a comprehensive approach is taken, the following subject areas should also be considered:

(1) Pre-event focus of remediation planning:

- Doctrine: policy, procedures, guidance, and agreements with internal and external tenant commands/agencies
- Organization: structure and location
- Training: formal, informal, situational
- Material: physical, cyber, financial resources, redundancy
- Leadership: education, knowledge, and experience
- Facilities: physical, access, security, resiliency

(2) Basic steps to building an effective remediation plan are as follows:

(a) Confirm Stakeholders, Prioritize Risk, and Identify Options. It is important to identify asset owners, mission owners, and other stakeholders that have vested interest in remediating risk to mission assets. USMC-APM and/or MC-CAMS Next Generation will be used to prioritize risk to critical assets, as well as to prioritize impact of critical assets on all the missions supported by the asset. These systems generate priority values based on impact to mission and probability of occurrence. Remediation efforts will focus on obtaining optimal risk reduction and the most effective/efficient use of resources.

(b) Analyze Options and Determine the Best Approach. This step focuses on option analysis that determines the option with the most "bang for the buck" should a potential theat or hazard occur. Use of the USMC-RA tool or MC-CAMS Next Generation will assist MA personnel in analyzing options and determining the best remediation action(s). Executive level planing groups will should perform a cost-benefit analysis to balance risk to the asset and/or mission with the resource requirements necessary to execute the remediation action. In analyzing options to remediate or reduce risk of loss to identified assets, the following minimum elements must be considered:

i. Identify asset(s) covered by remediation plan;
ii. Identify mission criticality or impact score for each asset;
iii. Identify highest asset risk rating (which accounts for criticality, most likely T/H, and most significant vulnerability);

iv. Identify cost of risk remediation COA;
v. Identify revised risk rating rating should remediation COA be implemented; and
vi. Document COA selection.

An example of a Risk Remediation Analysis Matrix is Figure 3-3:

Figure 3-3:

Crical Asset	Vulnerability Rating	Risk Rating	Priority	Proposed Remediation Measures	Revised Vulnerability Rating	Revised Risk Rating
Asset A	High	Medium	3	Establish an alternate path for access to the DISN and/or the GIG.	Low	Low
Asset B	High	High	1	Use CCTV to search tops of vehicles prior to entry: screen search procedures from othr drivers; Harden commercial vehicle gate by installing removable bollards; Ensure MWD are used more frequently as a RAM.	Low	Low
Asset C	Critical	Medium	2	Consider establishing an alternative feed from power supply G. Procure & install back-up power generation at Asset E. Increase staffing at installation ECPs and purchase explosive detection technology to ensure security force has the appropriate tools and mapower to effectively detect explosives.	Medium	Low

(c) Develop and Coordinate the Remediation Plan. This step requires a plan of action and milestones (POA&M) be developed that details what needs to be done, how it is to be done, who is involved, and when will remediation be completed. The plan must include such elements as: criticality assessment, threat/hazard assessment, vulnerability assessment, risk assessment, risk management decision, resource requirments, stakeholder actions and impact.

(d) Implement the Remediation Plan. Once the plan is approved, track the milestones developed in the above POA&M and measure success. Remediation plan effectiveness can be assessed during the command's annual MA exercise or by higher headquarters mission assurance risk assessments; such as MCMAA.

(e) Execute Follow-Up Actions. These actions may include annual self assessments or other follow-up risk assessment to consider new missions and threats associated with command assets.

(3) Documentation. All remediation plans will be documented in MC-CAMS for information sharing purposes.

b. Mitigation. Mitigation is defined as actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure. Mitigation planning focuses on post-event actions and activities with the intent to respond to, or lessen the impact of the event on command assets and operations. Again, mitigation planning can be done by selected members of the MA Working Group or by the establishment of a command remediation/mitigation planning team. As part of risk management, commands should evaluate mitigation strategies to reduce risk and support command risk response objectives. The following discusses the mitigation planning process or steps and the types of mitigation plans:

(1) Mitigation Planning Process/Steps

Step 1. Develop mitigation goals and objectives. These goals and objectives must be mission-focused, considering the command's METs to include identified conditions and standards for execution. Mission focus helps in the prioritization of time and resources in Step 2.

Step 2. Identify and prioritize mitigation actions. This step involves identifying potential course of action that will reduce risks while supporting optimum cost-benefit strategies. All stakeholders need to be consulted during this step to ensure consideration of all equities and impacts. This step captures the responsible organization for executing the mitigation, the funding source and timeframe for completion.

Step 3. Prepare and document an implementation strategy. An implementation strategy is required because there may be many complex variables associated with developing, funding, procuring, training appropriate personnel, and coordinating mitigation measures with other existing security measures. Often, implementation requires a phasing approach that cuts across numerous commands, agencies, and stakeholders, creating a need for sychronization of priorities. It is recommended that the mitigation implementation strategy be exercised in some format to ensure desired results are achieved and any negative cascading affects are identified and addressed.

Step 4. Implement the plan and monitor progress. Commands will document their mitigation plans in MC-CAMS and CVAMP, as required by DOD policy. Also, commands will take every opportunity to measure the effectiveness of their mitigation plans through annual exercises and scheduled risk assessments.

(2) Types of mitigation plans/ or planning required. When mitigating risks to command mission assets and supporting infrastructure, the planning process must include the development of the following plans:

- Installation Emergency Response Priorities. This plan establishes first responder emergency response priorities with a focus on mission continuity. See Enclosure 2 for sample Emergency Response Priority Plan.

- Utilities Restoration Priorities. This plan identifies the priority of work for restoring utility infrastructure (e.g., electricity, POL, water) that specifically supports critical asset operations when utility systems are disrupted or destroyed. Priority restoration plans should be identified for critical assets, including those critical assets owned by tenant commands within the overall host installation priority planning.

- Installation Security Response Priorities/Plans. These plans address actions taken in concert with threat/hazard indications and warning, necessitating an escalation in security response. An example of these plans is the Security Force Augmentation Plan, Random Antiterrorism Measures Implementation plan, Force Protection Action Sets Plan. Security response and protection measure priorities should be identified for locations housing critical assets, including those critical assets owned by tenant commands within the overall host installation security response priority planning.

- Continuity of Operations Plans. See Marine Corps Order 3030.1.

- Reconstitution Plans.

c. Acknowledgement of Risk. After review of the risk assessment data, if commanders deem the overall risk to mission critical assets and high value assets to be acceptable, he/she can elect to forego remediation and mitigation planning and the implementation of security countermeasures. It is the commander's prerogative to acknowledge risk where appropriate in the Commander's judgment which is based on being fully informed of all risk assessment data. Historically, reasons for accepting risk revolve around cost-benefit analysis results, lack of resources to implement a desired risk reduction measure, or lack of a significant threat or hazard.

d. Capability Assessment. A Capability Assessment is a command, or unit-level evaluation (assessment) to identify capabilities for responding to a natural or manmade disaster or hazard. All installations shall conduct capability assessments and consider contingency planning activities. The objectives of the capability assessment are to:

(1) Consider the range of identified and projected response capabilities necessary for responding to any type of hazard.

(2) List installation resources by type to provide an asset capability report.

(3) Review policy, guidance, and planning documents to identify the organization's mission essential tasks (METs) and functions assigned to the organization.

(4) List installation personnel with an MET EM responsibility as identified in enclosure 3, paragraph 4.c of DoDI 6055.17.

(5) Identify costs associated with assessment outcomes for future budget planning.

3004. RISK MANAGEMENT PROCESS REVIEW. Once the risk management process is complete, it is essential that a thorough review of the overall process be conducted. This is typically done during the annual program review. This section discusses the components of the risk management review process.

a. Refine Plan. Necessary revisions to the AT plan can be documented and initiated during this portion of the process. As noted, the risk management process must be executed as a cycle. By using this framework, revisions can always be pursued and the AT program can always be improved.

b. Coordinate with Stakeholders. Stakeholders in the military and local civilian communities should be involved in the process review stage of the risk management process. This collaboration will ensure that supporting plans align with the risk management process. Stakeholders from the local community can also identify strengths and weaknesses, focusing on collaboration between the military and civilian agencies. Complex operating environments magnify the importance of coordinating with expeditionary forces. In order for expeditionary ATOs to effectively manage risk, they should possess a solid understanding of the local customs, culture, and society in which they operate. Interfacing and coordinating preventive and/or response measures with local stakeholders may ensure a more robust AT program. Coordinating with local stakeholders, however, should never be done at the risk of endangering the Marine Corps force or its mission.

c. Exercise and Modify Plan. The final stage in risk management process review is to execute the plan and make adjustments as needed. Once the all-hazards risk management plan is implemented and seen in motion, flaws may be identified that could not be comprehended during the planning process. If this occurs, immediate modification should be pursued.

CHAPTER 4

INFORMATION FUSION

CHAPTER 4

INFORMATION FUSION

4000. GENERAL. This chapter focuses on the concept of information fusion between military agencies and civil authorities as it pertains to AT. The process of sharing information among various organizations maximizes threat awareness, which will aid in developing the threat assessment as part of the AT risk management process. Information fusion may be pursued for immediate emergencies, imminent risks, or for routine operations. Whenever any threat information is wanted, commanders and Antiterrorism Officers (ATOs) must consult officials from the Naval Criminal Investigative Service (NCIS), Marine Intelligence, and the Staff Judge Advocate to obtain the most current procedural and legal guidance. Intelligence-related regulations and procedures must be followed when requesting threat information, collaborating with outside agencies and host nations, and/or reporting or disseminating threat information.

4001. NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS). NCIS is the Department of the Navy (DoN) component with primary responsibility for law enforcement and counterintelligence. It is the point of contact for all threat information requests per DONI. NCIS works to ensure the availability of accurate and timely intelligence necessary to successfully accomplish the DoN and Marine Corps mission. NCIS is also charged with satisfying requests for essential elements of information (EEIs) from tenant units aboard installations in the United States. Requests for NCIS support may be initiated by any commander, commanding officer, or other appropriate command authority in the DoN or Marine Corps. NCIS responsibilities include the following intelligence-related tasks:

1. Coordination with appropriate U.S. and host-nation agencies. As a member of the Department of Defense's (DoD's) Law Enforcement and Counterintelligence Community, NCIS provides law enforcement liaisons who interact with other federal, state, and local law enforcement agencies. NCIS is exclusively assigned to all criminal, investigative, counterintelligence, and security matters with law enforcement, security, and intelligence agencies for the DoN. NCIS is responsible for assisting the Federal Bureau of Investigation (FBI) or host-nation authorities with intelligence matters after terrorism incidents. NCIS also acts as the DoN liaison to host-nation agencies to exchange terrorist-related information. It should be noted that the

duties of NCIS do not restrict DoN and Marine Corps commands from conducting normal liaisons with federal, state, local, or foreign law enforcement officials in routine law enforcement matters such as traffic, physical security, minor crimes, and training.

2. Counterintelligence (CI). Under its counterintelligence mission, NCIS is responsible for ensuring that DoN and Marine Corps component commanders are apprised of NCIS CI activities through the cognizant Staff Counterintelligence Officer or CI/HUMINT Officer and for providing any intelligence reports or CI/Counterterrorism information that could impact DoN and/or Marine Corps forces.

3. Maintain a 24-hour operations center to receive and disseminate worldwide terrorist threat information. The Secretaries of the Military Departments ensure a capability exists to receive, evaluate (from a service perspective), and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Under the DoN, the Navy's Multiple Threat Alert Center (MTAC) and the Marine Corps Intelligence Activity (MCIA-OCONUS) were established to monitor foreign intelligence and CI activities focusing on terrorist groups and terrorist actions. NCIS oversees the MTAC, which serves as the fusion point and production center within the DoN for all terrorist, criminal, cyber, and CI information indicative of a threat to DoN assets throughout the world. The MTAC processes real-time information and operates on a 24-hour basis to provide commanders with a timely and common operational picture of security threats and vulnerabilities to reduce risks to Marine Corps forces and assets.

4. Provide commanders with information on terrorist threats concerning their personnel, facilities, and operations. NCIS will collect and disseminate foreign and, to a very limited extent, domestic, terrorist-related information to supported installations and activity commanders. Periodic international terrorism products and other threat data may also be provided to support commanders from NCIS. On request, NCIS will provide current intelligence data on terrorist groups and disseminate time-sensitive and specific threat warnings to appropriate commands. NCIS is also capable of conducting terrorist threat information briefings for working groups. NCIS can also answer specific RFI's if requested.

5. Oversee participation in the FBI National Crime Information Center (NCIC) System. NCIS is responsible for Marine Corps use of the NCIC System, and will enter all pertinent information for investigations. The NCIC is a computerized information system established for use by federal, state, and local law enforcement agencies. Through NCIC, users have the ability to access and extract information on wanted persons, stolen vehicles, license plates, guns, stolen identifiable articles, and the Interstate Identification Index.

NCIS serves as the Federal Service Coordinator (FSC) for the Marine Corps and is responsible to the FBI for all records entered by the Marine Corps as required. NCIS, as the FSC, is also responsible for records validation, quality control, dissemination of manuals and other NCIC publications, security, user training, audits, and any problems concerning system use. Installation Provost Marshals must access NCIC through the host state and abide by the state standards.

4002. MARINE INTELLIGENCE. Marine Corps intelligence components are those units, organizations, staffs, and offices that perform any intelligence activity, including collection, production, retention, or dissemination of intelligence information. Based on MCO 3800.2B, "Oversight of Intelligence Activities," Figure 4-1 provides the components of Marine Intelligence:

a. HQMC Intelligence Department.
b. Marine Corps Intelligence Activity (includes all subordinate commands/elements).
c. Unit G-2/S-2 staffs.
d. Intelligence battalions.
e. Radio battalion.
f. Reconnaissance battalions/companies.
g. Scout sniper platoons.
h. Unmanned Aerial Vehicle squadrons.

Figure 4-1. Components of Military Intelligence

Marine Corps Intelligence is a crucial asset for Marine Corps commanders and ATOs in an expeditionary environment. Due to strict policy governing intelligence dissemination and collection, it is essential that the fusion between AT planning and intelligence be provided oversight on CONUS installations. Appropriate guidance should be pursued and proper channels should always be followed when trying to obtain intelligence data. At the installation level, NCIS, explained in the preceding section, will maintain communication with Marine Intelligence personnel to provide commanders with real-time intelligence pertinent to AT. At an expeditionary level, commanders will have direct involvement with intelligence units for war-fighting functions.

1. Intelligence within the AT Plan. Annex B of the AT Plan provides overarching intelligence guidance for the plan. This annex supports the commander's intent by coordinating the intelligence functions that provide support to AT issues. Additionally, Annex B outlines methods and procedures for the receipt, collection, and dissemination of sensitive or classified AT information during all three main phases of operations. It serves as a guide for tenant units to execute the coordination required for the collection and dissemination of threat information, and describes the unit/personnel responsibilities involved in handling such information. Within Annex B, the Commander must circulate among the lead intelligence agencies involved and the system in place to access current intelligence. Once this information is established, Marine Corps commands can request threat information as needed and receive a local threat picture. Location (CONUS or OCONUS) ultimately determines the participants involved with intelligence collection and dissemination. **In-theater,** national-level agencies, Combatant Commanders, and intelligence systems provide threat information. **In the United States,** local installations must acquire the local terrorist threat information by querying the FBI through NCIS. Installation commanders should also strive to maintain situational awareness

by utilizing open source information and other information sources.
Figure 4-2 outlines the mandatory components of the Intelligence Annex in an AT plan.

ANNEX B	-	Intelligence [Enter the agency(ies) responsible for intelligence and specific instructions]
Appendix 1	-	Local Threat Assessment
Appendix 2	-	Local WMD Assessment
Appendix 3	-	Local Criticality/Vulnerability Assessment
Appendix 4	-	Risk Assessment
Appendix 5	-	Pre-deployment AT Vulnerability Assessment

Figure 4-2. Annex B Composition as structured in DoD 2000.12H

2. Priority Intelligence Requirements (PIR) and Commander's Critical Information Requirements (CCIR). Also found in Annex B, PIRs are intelligence requirements associated with a decision that will critically affect the overall success of a command's AT mission. PIRs constitute the commander's guidance for the intelligence collection, production, and dissemination efforts and are a subset of CCIRs. It is essential that sound PIRs and CCIRs are placed in the AT Plan, as they assist with identifying and filling in information and intelligence gaps. Additionally, PIRs and CCIRs are circulated to prioritize the dissemination of valuable information up the chain of command. If there is a need to obtain additional or new information, PIRs and CCIRs should be adjusted as necessary. CCIRs are discussed in more detail in FMFM 6-1, *The Marine Division.*

3. Marine Corps CI/HUMINT. Service Counterintelligence (CI) and Human Intelligence (HUMINT) (CI/HUMINT) are a single source capability for the Marine Corps. Marine CI/HUMINT resources are assigned to the Operating Forces and to the supporting establishment to perform CI/HUMINT missions in support of Commanders in wartime, peacetime, and contingency operations.

Marines conduct CI operations, activities, and functional services in order to identify, track, locate, neutralize, and counter the effects of hostile intelligence and terrorist activities that threaten Marine Corps forces, operations, and installations.

The vast majority of Marine Corps CI operations and activities will be conducted at installations or operational areas outside the continental United States (OCONUS) and in support of

operating forces assigned to COCOM. For OCONUS exercises, operations and contingencies, Marine CI/HUMINT assets, in coordination with NCIS, normally deploy in advance of the main force in order to collect current threat information and provide intelligence support to AT/FP operations.

4003. FUSION PROCESS. The ability to acquire and analyze suspicious activity reports for indications of possible pre-attack terrorist activities is a critical component of intelligence support to force protection. Department of Defense Instruction (DoDI) 2000.16 tasks the Marine Corps to develop a process through which to "integrate and fuse all sources of available threat information from local, state, federal, host-nation law enforcement agencies." As mentioned previously, one of the main functions of NCIS is to liaise with local law enforcement agencies and to investigate all criminal and CI activity. The goal of the Commander and the ATO (with NCIS assistance) as related to intelligence and information fusion is to collect available information and combine with internal/external resources to create a baseline threat picture that can serve as the foundation of the threat assessment outlined in Chapter 3.

Many state fusion centers have been established, along with regional JTTF cells, to help provide a regional location for information sharing. The Secretary of Defense (SECDEF) directed suspicious incident reporting to be inputted into the FBI Guardian database for CONUS. NCIS is the conduit for inputting these reports. The FBI is responsible for validating and investigating all inputs into Guardian.

4004. SURVEILLANCE DETECTION. Installation AT programs should integrate surveillance detection (installation responsibility) and counter-surveillance (law enforcement/NCIS responsibility) programs. Organic surveillance detection capability should be indentified in the AT plan. If an organic capability does not exist, the Commander must arrange for support from HHQ or another entity. Surveillance detection should include the identification of surveillance requirements, the identification of hostile surveillance locations, and an established information fusion process for suspicious activity. To neutralize surveillance, ATOs should liaise with law enforcement and counterintelligence entities and develop appropriate surveillance responses to include RAMs, FPCON increases, and awareness briefs. It is strongly recommended that a community

watch program is implemented and reporting procedures on suspicious activities are widely known.

4005. ACTIVITY REPORTS. To minimize the risk of potential threats and provide a more comprehensive picture of current trends, techniques, and procedures of emerging threats, as well as develop a more thorough threat assessment picture at the installation level, an incident-reporting and information-sharing mechanism should be in place throughout all command levels. To achieve greater success in mitigating risks and diminishing potential threats, the information-sharing process must be coordinated and enforceable, with each command level sharing responsibility.

1. Commanders. It is recommended that commanders develop comprehensive PIRs/CCIRs that support the collection requirements regarding gaps in intelligence and information on antiterrorism activities. NCIS agents and ATOs should be given clear guidance and responsibilities to facilitate the gathering of threat information and to maintain a thorough and updated threat assessment.

2. ATO. An ATO will liaise with the locally assigned NCIS agents through their information fusion cells, who will be responsible for the collection and dissemination of all information related to suspicious activities and incidents that occur within their area of operation (AO) and within their area of interest (AOI). The activity report will consist of the activities and incidents that are derived from the commanders' PIRs/CCIRs and/or from a list contained in Figure 4-3 below. The ATO is responsible for further dissemination of the report.

- **Non-Specific Threats**. Threats received by any means that do not contain a specific time, location, or area for an attack against U.S. forces, facilities, or missions. This includes any event or incident, or series of events or incidents, which in and of themselves may indicate the potential for a threat to U.S. forces, facilities, or mission, regardless of whether the threat posed is deliberately targeted or collateral.
- **Surveillance**. Any reported possible surveillance in which an attempt to record information or to use unusual means to monitor activities is observed. Such attempts may include use of cameras (either still or video), note taking, annotated maps or drawings, hand-drawn maps or diagrams, use of binoculars or

other vision-enhancing devices, or any reports from host-nation force protection of possible surveillance of U.S. assets.

- **Elicitation.** Any attempts to obtain security-related or military-specific information by anyone who does not have the appropriate security clearance and the need to know. Elicitation attempts may be made by mail, fax, telephone, computer, or in person.

- **Tests of Security.** Any attempts to measure security reaction times or strengths; any attempts to test or to penetrate physical security barriers or procedures; any attempts to acquire or duplicate uniforms, badges, passes, or other security-related documents.

- **Repetitive Activities.** Any activities that meet one of the other TALON criteria and have occurred two or more times—the same activity by the same person and/or vehicle, within a 1-month period.

- **Bomb Threats.** Communication by any means specifically threatening to use a bomb to attack U.S. forces, facilities, or missions.

- **Suspicious Activities/Incidents.** This category should only be used if the information does not meet any of the above criteria. Any activity/incident that does not specifically fit into the aforementioned six categories, yet is believed to represent a force protection threat, should be reported under this category. Examples of this include issues resulting in the scrambling of homeland defense assets; thefts of material that could be used to manufacture false identification cards; thefts of military uniforms that may be used to gain access to a military installation, etc.

- **Be on the Lookout (BOLO).** Notifies other organizations of a particular individual or vehicle involved in a force protection incident. This information allows other installations/organizations to take proactive countermeasures against a potential threat.

- **Vehicle Turnarounds.** Captures information about vehicles and its occupants who are denied entrance to DoD installations. Multiple vehicle turnarounds may meet the criteria for repetitive activity, and therefore constitute a TALON event.

- **Other Incidents.** Used to record additional force protection-related information that is not included in any of the other force protection categories.

- **Non-Event.** Used to close a redundant or erroneous event.

Figure 4-3. Suspicious Activity Report Events/Incidents

The reporting of activities in and around the installation will ensure that ATOs and NCIS agents are coordinating with local law enforcement agencies on a continual basis and will help to foster better working relationships and information sharing with external agencies. The ATOs and NCIS agents should attend/participate in the FBI Field Intelligence Group (FIG) meetings within their region(s) for additional threat information. The activity report will then be submitted to their higher command (MCI East/West Fusion Cells or equivalent). The MCI/Higher Headquarters' (HHQ's) fusion cell will assemble all of their installation reports and forward them to the MFN Fusion Cell for further collection, database entry, and analysis.

a. Intelligence Oversight. In accordance with Executive Order 12333, DoD has established procedures in DoDD 5240.1 and DoDD 5240.1-R for the collection and retention of information concerning U.S. persons. The activity report will collect information on the actual event or activity. It will not provide information on U.S. persons, groups, or organizations. NCIS will ensure all criminal activity and information on U.S. persons is vetted and stored separately.

3. Information Fusion Cell. It is recommended that a regional information fusion cell be established at the respective Marine Corps commands or through one of the intelligence units in their subordinate commands. The information fusion cell led by the local NCIS agent, assisted by an ATO and an intelligence analyst, should assist local installations with their threat assessments and activity reports, to liaise with regional JTTFs and FBI FIGs, and to coordinate with the component command intelligence fusion cell.

4. Intelligence Fusion Cell. It is recommended that the Intel Fusion Cell, along with the ATO, oversee the timely collection of all activity reports. The Intel Fusion Cell should ensure all incidents and activities from the reports are shared and stored through various national agency programs (MTAC, CIFA, Guardian, etc.). In addition, the Intel Fusion Cell should ensure that all activity reports are in accordance with DoDD 5200.27. The Intel Fusion Cell should use various national law enforcement and intelligence agencies to integrate all threat information, intelligence, and CI information to produce a comprehensive

threat picture that facilitates the risk management process. The Intel Fusion Cell will coordinate with the AT Program Manager and recommend convening a Threat Working Group as needed. The Intel Fusion Cell will also provide the Major Subordinate Commands (MSCs) and ATOs with relevant data for the development and procurement of their respective Local Threat Assessments and timely dissemination of threat warnings.

5. Activity Report. The objective of an activity report is to enhance the information fusion process by compiling activities that may otherwise go unreported or may not be sent to a higher command for collection and analysis. This reporting process will facilitate the development of critical relationships among the ATOs, NCIS, DoD, and non-DoD law enforcement agencies.

The format and frequency for activity reports are determined by the commander on the recommendation of the Intel Fusion Cell. At a minimum, the report for each event/activity should contain the information in Figure 4-4.

Activity Report

Reporting Command/Installation
Type of incident
Location
Date-time group
Summary of incident and/or law enforcement action

Figure 4-4. Report Format

CHAPTER 5

INCIDENT/EVENT RESPONSE AND MANAGEMENT CAPABILITIES

CHAPTER 5

INCIDENT/EVENT RESPONSE AND MANAGEMENT CAPABILITIES

5000. GENERAL. According to the National Response Framework (NRF) and DoDI 6055.17, Installation Emergency Management Program, emergency management (EM) is the coordination and integration of all activities necessary to build, sustain, and improve the capability to prepare for, protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other manmade disasters. The integration of activities must span four phases: Mitigation, Preparedness, Response, and Recovery. These four phases can be divided into three basic sections: Pre-incident (mitigation and preparedness), Incident (response), and Post-incident (recovery). Management of natural, man-made, and terrorist events is directed by the NRF and National Incident Management System (NIMS), which include guidance on Emergency Operations Center (EOC) and the Incident Command System (ICS).

5001. NATIONAL RESPONSE FRAMEWORK (NRF). The NRF establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The NRF incorporates best practices and procedures from incident management disciplines – homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector – and integrates them into a unified structure. The NRF provides the framework for how the Federal Government coordinates with state, local, and tribal governments and the private sector during incidents. Working in conjunction with NIMS and ICS, the NRF establishes protocols to help save lives and protect the health and safety of the public, responders, and recovery workers.

1. National Incident Management System (NIMS). NIMS provides a consistent nationwide template to enable all government, private-sector, and nongovernmental organizations to work together during domestic incidents. NIMS is a comprehensive national approach to incident management that is applicable at all jurisdictional levels and across all functional disciplines. NIMS provides a framework for interoperability and compatibility by balancing flexibility and standardization. It comprises several components that work together as a system to provide a

national framework for preparing for, preventing, responding to, and recovering from domestic incidents.

2. Incident Command System (ICS). USMC CONUS installations should have an ICS in place to respond effectively to an incident or event. The ICS allows users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents without being hindered by jurisdictional boundaries. The ICS also enables personnel from a variety of agencies to meld rapidly into a common management structure. This interagency coordination improves accountability, enhances communication, and avoids duplication of efforts.

a. An Incident Commander (IC), whose chief responsibility is to manage the incident according to an Incident Action Plan (IAP), directs an ICS. The ICS should comprise a Command Staff and General Staff. A Command Staff is responsible for public affairs, health and safety, and liaison activities in the incident command structure. A Command Staff may include an information officer, a liaison officer, and a public safety officer. An information officer develops and releases information about the incident to the news media, incident personnel, and other appropriate agencies and organizations. A liaison officer serves as the point of contact for assisting and coordinating activities between the Incident Commander and various agencies and groups. A safety officer develops and recommends measures to the Incident Commander for ensuring personnel health and safety and to assess and/or anticipate hazardous and unsafe situations. A safety officer also develops the Site Safety Plan, reviews the IAP for safety implications, and provides timely, complete, specific, and accurate assessment of hazards and required controls. The General Staff includes Operations, Planning, Logistics, and Finance/Administrative personnel. Operations staff members are responsible for all operations directly applicable to the primary mission of the response. Planning staff members are responsible for collecting, evaluating, and disseminating the tactical information related to the incident, and for preparing and documenting IAPs. Logistics staff members are responsible for providing facilities, services, and materials for the incident response. Finance and Administrative staff members are responsible for all financial, administrative, and cost analysis aspects of the incident.

3. National Planning Scenarios. Fifteen National Planning Scenarios have been coordinated by the Homeland Security Council (HSC) in partnership with the Department of Homeland Security (DHS). These all-hazards planning scenarios have been developed for use in national, federal, state, and local homeland security preparedness activities. The scenarios are designed to be the foundation for the development of national preparedness standards from which homeland security capabilities can be measured.

a. National Planning Scenarios

(1) Scenario 1: Nuclear Detonation - 10-Kiloton Improvised Nuclear Device

(2) Scenario 2: Biological Attack - Aerosol Anthrax

(3) Scenario 3: Biological Disease Outbreak - Pandemic Influenza

(4) Scenario 4: Biological Attack - Plague

(5) Scenario 5: Chemical Attack - Blister Agent

(6) Scenario 6: Chemical Attack - Toxic Industrial Chemicals

(7) Scenario 7: Chemical Attack - Nerve Agent

(8) Scenario 8: Chemical Attack - Chlorine Tank Explosion

(9) Scenario 9: Major Earthquake

(10) Scenario 10: Natural Disaster - Major Hurricane

(11) Scenario 11: Radiological Attack - Radiological Dispersal Devices

(12) Scenario 12: Explosives Attack - Bombing Using Improvised Explosive Devices

(13) Scenario 13: Biological Attack - Food Contamination

(14) Scenario 14: Biological Attack - Foreign Animal Disease (Foot and Mouth Disease)

(15) Scenario 15: Cyber Attack

b. Using the National Planning Scenarios: The National Planning Scenarios are broadly applicable and focus on a range of capabilities. In addition to providing the design basis for national preparedness goals and response capability standards, the scenarios can provide the design basis for exercises. They have been developed in a way that allows them to be adapted to local conditions. Although certain areas have special concerns - for example, continuity of government in Washington, DC; viability of financial markets in New York; and trade and commerce in other major cities - every part of the United States is vulnerable to one or more major hazards. The Marine Corps, with a large presence in communities across the nation, should use these National Planning Scenarios as a foundation for their planning and exercises.

c. It is highly encouraged that the all National Planning Scenarios be reviewed and incorporated into the installation's Mission Assurance planning effort. A complete explanation of the National Planning Scenarios and planning process can be obtained via the internet through the DHS website. Planning should be coordinated with the appropriate Marine Corps Installations Command, local communities, and state emergency management officials.

5002. EMERGENCY OPERATIONS CENTER (EOC). An EOC is the physical location at which an organization comes together during an emergency to coordinate response and recovery actions and resources. The EOC is where the coordination of information and resources takes place on an installation. The EOC is not the Incident Command Post (ICP) and does not provide on-scene incident management. The EOC provides support to the incident when requested, helps to coordinate those incident activities as directed, and collects/disseminates timely and factual information while ensuring the installation maintains the continuity of its operations.

1. EOC Structure. The structure of the EOC facilitates a unity of effort and, as described in the NRF/National Response Plan (NRP), should follow NIMS. NIMS supports response through the following elements of unified command: (1) developing a single set of objectives; (2) using a collective, strategic approach; (3) improving information flow and coordination; (4) creating common understanding of joint priorities and restrictions; (5) ensuring that no agency's legal authorities are compromised or

neglected; and (6) optimizing the combined efforts of all agencies under a single plan. Under NIMS there is no design, layout, or configuration for EOC facilities. The EOC can be organized in a layout by major disciplines, jurisdiction, ICS Command Staff Structure, Emergency Support Functions, or some combination thereof, as long as it meets the needs of the installation to manage an emergency. It must be able to perform the following core operations, no matter its structure: information gathering and recordkeeping, coordination, decision making, plan development, resource management, communications, recovery management. Each installation's EOC is managed by an appointed individual called the Senior Watch Officer (SWO). This individual's billet varies from installation to installation; some installations utilize the ATO as the SWO.

2. EOC Management. Management of the EOC is a strategic effort that ensures Mission Assurance during an incident. The on-scene Incident Commander will develop a strategic plan for handling response operations. The Emergency Manager will manage the EOC and ensure that proper coordination is established and maintained throughout the response and recovery phases of an incident. On installations, the Emergency Manager is the Executive Officer or the SWO. The EOC's strategic plan is in support of the installation's continuity of operations (COOP) and protecting personnel.

3. EOC Activation. The EOC should be activated as soon as the event warrants the need for decision making, resource management, and COOP on the installation. The Emergency Manager should develop criterion that identify the events or situations that require the EOC to be activated. Activation criterion should be listed in the EOP. By using an all-hazards approach to emergency management and assessments conducted on the installation, priorities can be established. The EOC level of activation can be established based on the risk to vulnerable assets and personnel on the installation.

5003. EMERGENCY OPERATIONS PLAN (EOP). The EOP describes how people and property will be protected in an emergency or disaster. The plan should include information from NIMS and the NRF/NRP. These documents outline the approach that the Federal Government encourages communities across the country to implement as many of these guidelines to create a balance of operations and coordination. An EOP should be written with input from all tasked organizations, and then exercised. The EOP should be developed from various assessments conducted for the

installation. Careful analysis of all assessments within the risk management process aid in determining what is easily threatened, what hazards are present or what hazards may arise, what is vulnerable, and what the risks are to the installation and its personnel. The plan should be reviewed and updated regularly. Figure 5-1 provides the primary elements comprised in a civilian EOP.

- Introduction
- Purpose
- Situation and Assumptions
- Concept of Operations
- Organization, Roles, and Responsibilities
- Administration and Logistics
- Plan Development and Maintenance
- Authorities and References
- Functional Annexes

  Specific or Situational (Examples)
  - Force Protection / Security
  - Communications
  - Resource Management
  - Mass Care
  - Public Health Emergencies
  - Evacuation and Shelter Plan
  - Hazardous Materials
  - CBRNE Emergency Response Plan
  - Terrorism Plan
  - Destructive Weather Plan
  - Forest Fires and Wildfire
  - Special Events

Figure 5-1. Key Elements of A Basic Civilian EOP

2. Installation Emergency Management Program (IEMP). Marine Corps installations' version of the EOP mirrors the civilian model outlined in Figure 5-1, but may contain installation specific information. Figure 5-2 provides examples of IEMP elements.

- General responsibilities of the EOC and the positions
- Identified planning groups
- Concept of Operations
- Installation plans
- Addresses agreements

- Identifies Training of EOC personnel and the conducting of exercises - Mass Notification - Specific Sections or Annexes Based on Vulnerabilities to the Installation

Figure 5-2. Example of IEMP Elements

3. Standard Operating Procedures (SOP). An effective EOC relies on written policies and procedures in place before an emergency occurs. Each EOC will have unique requirements, certain standard policies, and procedures developed for each installation.

4. Standard Operating Guidelines (SOG). Each position within the EOC should have guidelines to follow while executing their respective tasks. A guide can take the form of a checklist or smart book. This level of organization serves as a means to focus the effort of the EOC staff and facilitates documentation required during an emergency or event.

5004. EMERGENCY OPERATIONS CENTER (EOC) AND INCIDENT COMMAND POST (ICP) INTERFACE. The interaction between the EOC and the ICP is a two-way coordination process critical to the successful outcome of an event. The EOC functions mutually support each other. Through training, exercises, and lessons learned from past events, the coordination between the Incident Commander or ICP and the EOC can be carried out efficiently as long as each function understands the benefits that the other provides. The EOC and ICP communicate via formal and informal routes. Formal information includes ICS forms, Incident Action Plans, objectives or goals, and assignment of resources. Whereas informal information includes notes, photos, video, and direct communications from the ICP functional areas directly to the EOC functional areas (i.e., on-scene plans section communicating directly to the EOC plans section to coordinate resources for the next operational period). Regardless of the form of communication, communication is critical to the success of both incident mitigation and the EOC responsibility to maintain Mission Assurance.

5005. DEFENSE SUPPORT TO CIVIL AUTHORITIES (DSCA). DSCA involves DoD support that may be provided by Federal military forces, DoD civilians and contractor personnel, DoD agency and component assets for domestic emergencies, designated law enforcement, and others. There are four primary mechanisms by which DoD assists in a Federal response to a domestic incident: 1) at the discretion of the President, 2) at the request of another

Federal agency under the Economy Act, 3) in response to a request from the Federal Emergency Management Agency following a declaration of a national disaster or emergency under the Stafford Act, or 4) under the DoD immediate response authority. The second and third mechanisms require the Secretary of Defense to approve a request for assistance. The fourth mechanism refers to the authority that local military commanders and responsible officials of other DoD components possess to take necessary action to respond to requests from civil authorities. This authority is vested when imminently serious conditions resulting from any civil emergency or attack require DoD assistance to save lives, prevent human suffering, or mitigate great property damage. Although DoD is in a supporting role when providing assistance to civil authorities, at no time does the supported agency exercise any command and control over DoD forces. It is imperative that the Staff Judge Advocate is involved in DSCA planning.

5006. CONTINUITY OF OPERATIONS (COOP). COOP is the capability to maintain mission essential functions, tasks, or duties necessary to accomplish a military action or mission during an All Hazards event... COOP planning includes preparedness measures, response actions, and recovery activities planned or taken to ensure continuation of these functions. COOP planning is a part of the fundamental mission of Marine Corps Installations and Commands.

1. Planning. Though many of the concepts within COOP should be addressed within the EOP, special consideration to COOP warrants a separate plan. Additionally, subordinate commands and mission critical sections should develop action plans for each stage of COOP implementation. Figure 5-3 provides a list of the minimum planning requirements necessary for each stage of COOP implementation.

MINIMUM PLANNING REQUIREMENTS FOR EACH STAGE

- Decision Matrix for COOP
  - With warning
  - Without warning during duty hours and off duty hours
  - Notification
    - Of alternate facilities
    - To Higher Headquarters
    - of points of contact, as appropriate
    - of personnel (COOP essential personnel)

- Alternate Operating Facility Operations
  - Reception of COOP personnel
  - Transition of responsibilities to COOP personnel
  - Guidance for personnel
  - Identification of replacement personnel and augmentees
  - Execution of all essential functions at alternate operating facilities
  - Report to Higher Headquarters as to the alternate location, communications, and anticipated duration of relocation
  - Redeployment to primary facility and return to normal operations

- Transitioning from COOP to Normal Operations
  - Return to normal operating facilities
  - Report to Higher Headquarters
  - After Action review of COOP and submission of AAR to Higher Headquarters.

Figure 5-3. Minimum Planning Requirements

2. COOP Plans and Procedures. A COOP plan shall be developed and documented. Development of the Installation COOP should be the responsibility of the Installation G-3 or Director, Operations Division. When implemented, the plan will provide for continued accomplishment of an installation or command's essential functions under all circumstances. At a minimum the plan must:

a. Identify essential functions, activities, and resources needed to perform them.

b. Establish orders of succession to key command and installation positions, establish and maintain current roster(s) of fully equipped and trained COOP personnel with the authority to perform essential functions, and include a devolution or control plan.

c. Provide for the identification and preparation of alternate operating facilities for continuity operations.

d. Outline a decision process for determining appropriate actions in implementing COOP plans and procedures.

e. Provide procedures for the notification and relocation of COOP personnel to one or more alternate operating facilities.

f. Provide procedures for the orientation of COOP personnel and for conducting operations and administration at alternate operating facilities.

g. Provide for operational capability at the COOP site as soon as possible with minimal disruption to operations, but in all cases within 12 hours of activation.

h. Establish reliable processes and procedures to acquire resources necessary to continue essential functions and sustain operations until normal business activities can be reconstituted, which could be up to 30 days.

i. Provide for the ability to coordinate activities with non-COOP personnel.

j. Provide for reconstitution of Command or installation capabilities and transition from continuity operations to normal operations.

3. Training and Exercise. Validation of the plan is critical in order to ensure that all plans and goals of the COOP can be met. Annual exercise requirements should be used to exercise and validate COOP plans.

CHAPTER 6

REPORTING

CHAPTER 6

REPORTING

6000. GENERAL. The unpredictability of all-hazards incidents requires Antiterrorism Officers (ATOs) to be prepared at all times for any situation. If a significant situation arises, an ATO must be familiar with the proper channels to report the incident or event. This chapter provides guidance on several reporting channels that an ATO may need to use if an incident or event occurs. Familiarity with the reporting requirements for each of these channels is important to ensure the timely and accurate passing of information. Sharing information along the appropriate chain of command is crucial in ensuring HHQ possesses the necessary information to prevent, prepare, or provide support when an incident or event occurs.

6001. OPERATIONAL REPORT-3 (OPREP-3). OPREP-3 reports use of command post channels to immediately notify commanders of any significant event or incident. Submitting an OPREP-3 report neither changes nor substitutes for any other report required by other orders or directives. OPREP-3 reports must be reported in verbal and written format. A voice report must be provided to the Marine Corps Operations Center (MCOC) within 15 minutes of any event or incident, or within 15 minutes of becoming aware of any event or incident. At a minimum, the voice report must include the date, time, location, unit/installation/personnel involved, and a general description of the event or incident. In addition to the verbal report, an OPREP-3 written report must be provided within 1 hour of any event or incident, or within 1 hour of becoming aware of any event or incident. Supplemental reports should be submitted as required to make corrections and/or provide additional information.

As MCO 3504.2 explains, OPREP-3 reports should be categorized by event or incident according to their nature:

1. Reports to National Military Command Center (NMCC). This category includes any OPREP-3 report in which national-level interest has been determined. The originator sends these reports directly to the NMCC with the flagword "PINNACLE."

2. Reports to Services and Combatant Commands. This category includes any OPREP-3 used to notify the appropriate Service or Combatant Command of a significant event or incident where national-level interest is not indicated or has not been determined. Services and Combatant Commands monitor these

reports for national-level interest. Reports with national-level interest will be transmitted to the NMCC and all Combatant Commands with the flagword PINNACLE inserted into the identification line.

3. Combatant Command and Service Reporting Systems. Combatant Commands and Services may implement additional OPREP-3 reporting requirements that are not of national-level interest. The flagword PINNACLE will not be used in these reports. These reports may include:

a. OPREP-3 SERIOUS INCIDENT REPORT (SIR). This SIR provides the Commandant of the Marine Corps, through the MCOC, information about any significant event or incident that is not of national-level interest. An SIR may include an event or incident of a military or political nature, foreign or domestic, that involves Marine Corps personnel, units, or installations and that may result in a national or local official reaction, congressional interest, or media attention; an on-duty event or incident resulting in the death or disability of Marine Corps personnel or civilians, or resulting in at least $200,000 in property damage; an event or incident associated with a Marine Corps operation or training exercise that results in death; or a serious criminal event or incident that may result in foreign or domestic criminal jurisdiction over Marine Corps personnel and/or their dependents. Additional information on serious incident reports can be found in MCO 5740.2F.

b. OPREP-3 NAVY BLUE (NB). This NB report provides the Chief of Naval Operations, through the Navy Operations Center, information about any significant event or incident that is not of national-level interest.

c. OPREP-3. This report provides the Chief of Staff of the Army, through the Army Operations Center, information about any significant event or incident that is not of national-level interest.

d. OPREP-3 BEELINE or HOMELINE. This report provides the Chief of Staff of the U.S. Air Force, through the Air Force Operations Center, information about any significant event or incident that is not of national interest.

6002. BLUE DART. BLUE DART is an AT threat-warning program designed to disseminate time-critical threat warning information from the information collector to the threatened installation or

unit. A BLUE DART warning is only used when specific, valid, and credible information regarding a terrorist threat is available. BLUE DART can only be used when all of the following criteria are met: the time of the attack is known; the attack time is within 72 hours of threat information receipt; and the unit, individuals, or location to be attacked and the method of attack are known. BLUE DART should not be used to provide general warnings, report terrorist threats that have already occurred and passed, or report demonstrations, civil disturbances, or local bomb threats. An AT program should establish command-wide policy for threat-warning dissemination. The policy should adhere to BLUE DART-approved procedures and content. Enclosures 2 through 4 of Appendix H [Sample Separate AT Plan] contain additional information on BLUE DART procedures and content.

1. BLUE DART Procedures. When information meets the BLUE DART criteria, a warning should be passed through the fastest means possible and within 30 minutes of receiving the threat information. The targeted unit's duty officer should be immediately contacted by telephone, preferably through a secure phone. Non-secure communications may be used, but only when secure means are unavailable or judged to be too slow. If the sending unit is unable to contact the targeted unit by telephone, BLUE DART information should be immediately telephoned to the local major command.

After dissemination of the threat to the targeted unit, the originator must transmit a written follow-up message to appropriate commmands and to HHQ. Sharing threat information with higher commands keeps them informed of the situation and aids in helping to "connect the dots" if there is a larger threat developing.

2. BLUE DART Content. The initial telephone message must include the following information: this is a BLUE DART terrorist threat warning; the caller's identity, organization, and telephone number; the location of the terrorist attack; the time and date of the attack; and the method of attack. If known, the telephone message should also include the identity of the attacker(s), the type of weapon and method of attack, and the reason for the attack. The source of information should only be given if the message is delivered over secure communications.

The written follow-up message should adhere to the format outlined in Figure 6-1.

FM (Sending unit)
TO (Targeted unit)
INFO AIG 988
(Other commands deemed appropriate)

Classification: _____-
SUBJ/BLUE DART
1. Threat: Specific information concerning terrorist attack, which will include the following:

   a. Specific unit location or person to be attacked. (mandatory)
   b. Specific time and date of attack. (mandatory)
   c. Identity of attackers. (if known)
   d. Identity of type of weapon (bomb, rifle, etc.) to be used and the method of attack. (mandatory)
   e. Provide the reason for the attack. (if known)

2. Source: Original information source; provide source description, access, and assessment of source's reliability.

3. Chronology: Events since receipt of information, including notification of affected unit.

4. Originator: Identity of individual who initially acquired the information, time information was obtained, and telephone number(s) of the message sender's command center or watch.

Figure 6-1. Blue Dart Follow-Up Message Format

6003. UNFUNDED REQUIREMENTS (UFRs). UFRs are validated, documented, and prioritized documents that did not receive funding via the Combating Terrorism Readiness Initiatives Fund (CbT-RIF) or the Combatant Commanders Initiative Fund (CCIF). If the component is unable to fund the requirement(s), a well-documented UFR should be forwarded to both the Combatant Command and the Service AT staff for consideration. The Combatant Command staff members are responsible for consolidating UFRs and including them in the Combatant Command's Integrated Priority List submitted to the Office of the Secretary of Defense (OSD) in October and November. Combatant Commands are then required to forward the consolidated UFR list to the Joint Staff for coordination and prioritization. OSD will review the budgets proposed by the Services to meet AT objectives during the Planning, Program, Budgeting, and Execution (PPBE) Review.

6004. HIGHER HEADQUARTERS (HHQ) REPORTS. In addition to UFRs, other reports, such as vulnerability mitigation reports and exercise after-action reports (AARs), must be sent to HHQ.

1. Vulnerability Mitigation Reports. Once a Joint Staff Integrated Vulnerability Assessment or other vulnerability assessment has been conducted, a vulnerability mitigation report should be drafted that details all vulnerabilities and all actions being taken to mitigate them. All vulnerability assessment results must be entered in CVAMP within 120 days from the completion of the asessment. Where vulnerability assessment reports involve a critical asset within the meaning of the DOD and Marine Corps CIP, remediation or mitigation actions undertaken with respect to vulnerabilities and risks to critical assets must also be uploaded to MC-CAMS. Appendix P [Sample Vulnerability Mitigation Report] contains an example and additional information on creating Vulnerability Mitigation Reports.

2. After-Action Reports (AARs). In accordance with MCO 3504.1, all Marine Corps commands and activities must submit AARs for all major exercises to the Marine Corps Center for Lessons Learned (MCCLL). Disseminating AARs is important for two reasons: (1) dissemination allows other Marine Corps entities to benefit from these operational experiences, and (2) AARs can be used by advocates and proponents to support important changes to the Marine Corps AT program. AARs may be submitted electronically via the MCCLL Web site at

http://www.mccll.usmc.mil for unclassified information, or at http://www.mccll.usmc.smil.mil for classified information.

3. Combating Terrorism Readiness Initiative Fund (CbT-RIF). CbT-RIF is an emergency funding line designed for emergent high-priority combating terrorism requirements. When emergency funding is needed and all CbT-RIF requirements are met (see Chapter 9, Resource Application and Funding, section 9004.3, for a detailed explanation of CbT-RIF), a CbT-RIF request is developed and submitted via Core Vulnerability Assessment Management Program. All CbT-RIF requests should be submitted to HHQ for visibility. The Security Division within Plans, Policies, and Operations of Headquarters Marine Corps will work with the Deputy Commandant of Installations and Logistics to resolve any CbT-RIF-related issues that may arise.

CHAPTER 7

ANTITERRORISM TRAINING

CHAPTER 7

TRAINING

7000. GENERAL. The cornerstone of the Marine Corps AT program and the best deterrent against terrorism is an alert, educated, combat-ready Marine. To achieve sufficient AT awareness, a thorough, dynamic, and integrated training program has been developed to ensure all Marines, family members, and civilian employees receive appropriate instruction relative to their grade/position, location, and the terrorist threat. It is the Commander's duty to ensure all personnel receive appropriate AT training to advance AT awareness. Commanders must also establish a process that provides personnel with appropriate and timely AT training, that collects and reports information on personnel received within the command who have not completed the required Level I training, and that maintains and updates individual records. Formal Marine Corps AT training includes Level I through Level IV AT training and Area of Responsibility (AOR)-specific training. This chapter, in addition to describing the formal Marine Corps AT training courses, details several other training programs that may be beneficial to AT personnel. The Training Management Module within Marine Online may be utilized to track training. The transactions reported on the Training Management Module are stored in the Operational Data Store Enterprise (ODSE) and allow Commanders and Higher Headquarters to identify trained personnel. Specifically, the Training Management Module tracks mandatory annual Level I AT Awareness training and identifies Level II and III trained personnel.

7001. AT LEVEL I. AT Level I is the initial AT awareness training course for all Marine Corps personnel. As directed in Department of Defense Instruction (DoDI) 2000.16, all Marine Corps personnel will receive AT awareness training during initial service entry. At a minimum, a qualified AT Level II-trained individual must teach the AT Level I course. Standard 25 of DoDI 2000.16 outlines the requirements for AT Level I training. Level I training includes the following topics: an introduction to terrorism; terrorist tactics and operations; individual protective measures; personal protective measures for CBRNE attacks, including sheltering in place, evacuation, indicators of a CBRNE attack, and impromptu methods of decontamination; terrorist surveillance techniques; improvised explosive device (IED) attacks; kidnapping and hostage survival; and an explanation of terrorism threat levels and Force Protection Condition System levels and measures.

1. All Marine Corps personnel and civilian employees will receive AT Level I awareness training at least annually if they are deployed, eligible for deployment, or if the terrorism threat level in the United States and its territories rises above moderate. All active duty Marines will also receive AT Level I awareness training at least annually.

2. Web-based AT Level I awareness training is currently available at http://www.at-awareness.org. The access code is "AWARE" (no quotes). Proceed by creating a self-generated user ID and password. Upon completion of the training, print the completion certificate and forward it to your ATO and command training officer for placement in your official record.

3. Family members of Marine Corps personnel and civilian employees 14 years of age or older traveling overseas on official business will receive AT Level I awareness training. Furthermore, all family members should be encouraged to receive AT Level I awareness training before any overseas travel.

4. Marine Corps contractors will be offered AT Level I awareness training under the terms and conditions specified in the contract.

7002. AT LEVEL II. AT Level II training is designed to instruct and certify an appointed ATO. Every installation, separate facility, stationary unit, or deployed unit of more than 300 personnel throughout the chain of command (battalion, wing, squadron, equivalent-sized units and above) is required to have at least one Level II-certified ATO. The Commander of an installation/unit will assign the ATO in writing and will ensure the ATO completes AT Level II training. Graduates of the Level II training will have the requisite knowledge and materials necessary to manage a comprehensive Installation/Unit AT program and advise the Commander on all AT-related issues. DoDI 2000.16 outlines the requirements for Level II training, which include understanding AT roles and responsibilities; the minimum required AT program elements; how to organize AT groups; risk management principles; how to develop an AT plan; and how to create and execute an AT program. IAW MCO 3302.1E, procedures must be developed for identifying Level II trained personnel via the Marine Corps Total Force System (MCTFS).

7003. AT LEVEL III. Level III AT training is a pre-command course offered at the Commanders' Course in Quantico, VA. It is

designed to provide Marine Corps commanding officers and prospective commanders with the necessary skills and knowledge to direct their command's AT program. In particular, Level III training will provide prospective commanders the depth and body of knowledge necessary to perform the full spectrum of AT responsibilities. This training should include instruction on the overall AT duties and responsibilities of the Commander, AT program elements, AT plan development, AT working groups, and how to build a sustainable AT program.

7004. AT LEVEL IV. AT Level IV training is an executive seminar that provides senior military and civilian leaders with a platform for focused updates, detailed briefings, and AT/consequence management war games. Level IV training is designed to enhance the prospective and decision-making considerations of senior leaders—O-6 to O-8 and civilian equivalents. It targets Commanders and personnel, including ATOs and Joint Task Force Commanders, who have AT policy, planning, and operations responsibilities. The Joint Staff Directorate for AT (DDAT/HD J-34) conducts the Level IV executive seminar. Its purpose is to create a senior-level forum for the presentation and discussion of prevailing AT issues as they affect military operations.

7005. AREA OF RESPONSIBILITY (AOR)-SPECIFIC TRAINING. The Service Component of a Geographic Combatant Command is responsible for protecting all assigned personnel in their AOR. Thus the Services Component of a Geographic Combatant Command must develop AOR-specific AT information to orient all deployed Marine Corps personnel and civilian employees. Deployed Marine Corps personnel will be periodically provided with an AOR update and threat brief that may be classified in nature. AOR-specific information should supplement, not replace, annual AT Level I awareness training.

1. ATOs assigned in a Geographic Combatant Commander's AOR will coordinate closely with AT representatives from the Component and Subordinate Commands to develop training materials that address AOR-specific issues. The topics should include the histories, tactics and techniques, and methods of operations of specific terrorist groups; self-protection measures; IED recognition; physical security measures for residents of housing units located off a Marine Corps installation; security measures for executives and their immediate staff; family security measures; and any other topics mandated by the Combatant Commanders.

2. Commanders will ensure personnel departing for or transitioning to a Geographic Combatant Commander's AOR are exposed to and execute the requirements of the gaining Combatant Commander's AOR update. This information will be available through the chain of command and may be provided through multiple means, including Combatant Commander publications, messages, and computer home pages.

3. To fulfill all pre-travel briefing requirements when traveling overseas, personnel must be briefed in accordance with the highest terrorism threat level established by the Department of Defense (DoD) or the AOR Combatant Commander for each individual country. Additional predeployment-specific AT training requirements, such as high risk of capture; code of conduct/survival evasion, resistance, and escape; or other training may be required. Therefore, required training should be identified and made available as soon as the requirement for travel becomes known.

4. Failure to understand and comply with briefing requirements in advance of travel requests may result in rejection of area/country clearance requests. Current terrorism threat level information for AOR Combatant Commanders may be obtained at the following numbers: JFCOM (800) 542-08646; CENTCOM (813) 828-6289/90/91; EUCOM 011-441-480-84-1414; PACOM (808) 477-7309; SOUTHCOM (888) 547-4025, extension 3720. The Defense Intelligence Agency also provides intelligence product and threat information via their classified Web site at http://www.dia.smil.mil/.

5. State Department travel advisories that reflect country-specific security concerns (terrorist, insurgency/political instability, criminal threat, etc.) may be obtained from the nearest State Department office, embassy, and/or consulate via the Internet (http://www.state.gov) or by calling (202) 647-5225.

7006. AT-RELATED TRAINING. In addition to the formal Marine Corps AT training courses, there are a number of additional training resources available to assist an ATO. The following training programs have not been validated by the Marine Corps Training and Education Command, but they may provide a valuable educational opportunity for ATOs.

1. Defense Threat Reduction Agency (DTRA) AT Program Mobile Training Team (MTT). DTRA MTTs provide a training session to inform AT personnel about their assessment process. Joint training environments expose personnel to the issues and lessons-learned from other services, as well as provide a forum to express service positions and initiatives at the Staff/AO-level. JSIVA MTTs are a means to continue the professional development for those who have not received formal USMC training on assessment methodologies/processes (vulnerability and/or risk-based). Typically, the sessions begin with an overview of the inspection process; focus groups are then arranged for personnel engaged in one of the five JSIVA classifications: terrorist operations, security operations, structural engineering, infrastructure engineering, and emergency management.

2. Dynamics of International Terrorism. The Dynamics of International Terrorism course provides selected personnel with a basic understanding of the theory, psychology, organization, technique, and operational capability of terrorist groups on an international and regional basis. This course is located at U.S. Air Force Base, Hurlburt Field, FL, and course duration is 5 days.

3. Federal Emergency Management Agency (FEMA) Courses. Marine Corps personnel with a reasonable likelihood of involvement in domestic incident management will be familiar with the NIMS, NRF, and the Incident Command System. FEMA's Independent Study Program offers online courses through the Emergency Management Institute (EMI) on each of these topics, as well as operational planning, disaster logistics, emergency and disaster communications, emergency operations center, continuity programs, hazard mitigation, and integrated preparedness. An ATO can access these courses at http://training.fema.gov/IS/crslist.asp. These training courses are vital to ensure ATOs possess the necessary knowledge to effectively operate with civil authorities during an incident.

4. Federal Law Enforcement Training Center (FLETC) Courses. FLETC serves as an interagency law enforcement training organization for more than 80 federal agencies. FLETC also provides services to state, local, and international law enforcement agencies. The Counterterrorism Division (CTD) of FLETC has several training courses and programs relating to terrorism methodology, threat response, and infrastructure protection. The CTD also operates a specialized AT/physical

security training facility. Courses taught by the CTD staff in the center's basic training programs include terrorism, critical incident response, weapons of mass destruction (WMD) and hazardous materials, physical security, operations security, and land transportation AT. In addition to basic courses, the CTD also offers advanced training programs to enhance the knowledge and abilities of today's law enforcement professionals to effectively manage an all-hazards environment. The center is headquartered at Glynco, GA.

5. Core Vulnerability Assessment Management Program (CVAMP) Training. CVAMP is a program that provides users with an automated means to meet the DoDI 2000.16 requirement to identify, track, and manage vulnerabilities throughout the chain of command. CVAMP provides the means to organize and prioritize identified vulnerabilities and track their status until they are mitigated. Thus the CVAMP program serves as a vehicle to highlight AT program shortfalls due to unmitigated vulnerabilities within the responsible chain of command. CVAMP is also useful for prioritizing AT resource requirements and submitting input into the Combating Terrorism Readiness Initiatives Fund and/or unfunded requirement process. ATOs should acquire CVAMP training to effectively use this program. The CVAMP community on ATEP in AKO offers training materials, including briefings, user guides, and a Web-based training module for ATOs.

6. Critical Infrastructure Vulnerability Analysis and Protection Training. The Naval Postgraduate School's Center for Homeland Defense and Security offers free non-credit courses online, including one on Critical Infrastructure Vulnerability Analysis and Protection. This course has not been formally sanctioned by the Marine Corps, but it teaches ATOs how model-based vulnerability analysis can support the drafting of AT policies and procedures. ATOs can find additional information on this course and others offered at the Naval Postgraduate School's Center for Homeland Defense and Security at: http://www.chds.us/?special/info&pgm=Noncredit.

7. MarineNet. MarineNet offers distance learning courses to all Marines - active duty, reserve, civilian, and retirees - and a number of courses to family members with valid government identification. It offers a diverse range of courses on military training and education, information technology, and personal growth and professional development topics. MarineNet provides detailed tracking of learning progress, 24/7 access to courses,

and the automatic passing of course completion and test results to the Marine Corps Training Information Management System (MCTIMS). MarineNet can be accessed at www.marinenet.usmc.mil/portal

8. Johns Hopkins Center for Public Health Preparedness (JHCPHP) Training. JHCPHP offers free on-line training courses under the Chemical, Biological, Radiological, Nuclear Terror module that provide instruction on preparedness responses to CBRNE events. The courses include Chemical Weapons and Water Safety; Introduction to Chemical Agents; Introduction to Weapons of Mass Destruction (Awareness and Intermediate Levels); Monitoring Chemical Agents; Practical Aspects of Preparing for, and Responding to, Radiological Terrorism; Radiation Terror 101; and Strategies for Prevention of Bombing Injuries. The courses may be accessed at: http://www.jhsph.edu/preparedness/training/online/index.html under the Chemical, Biological, Radiological, Nuclear Terror module.

9. Physical Security/Electronic Security Systems (ESS) Training. Physical security and AT are mutually supportive functions that must coordinate efforts to ensure a more robust security posture. Chapter 11 provides background on the physical security component of an AT program. In addition to working with the CIP Officer to incorporate physical security facets into an AT program, an ATO may pursue training courses to enhance his or her understanding of physical security.

a. All personnel assigned duties with a security force will meet the following minimal training requirements:

(1) The use and escalation of force and the safe handling of firearms, including issue and turn-in.

(2) Weapons training and qualification.

(3) Legal aspects of jurisdiction and apprehension.

(4) Mechanics of apprehension, search, and seizure.

(5) General and special orders and all aspects of the security force order.

(6) Use of security force equipment.

(7) Threat-specific training (e.g., vehicle bomb searches, terrorism awareness, WMD awareness).

b. Marine Corps site representatives will possess MOS 5814, Physical Security Specialist. ESS site representatives are the only personnel authorized to perform basic troubleshooting and first echelon maintenance, and will be trained and certified by the Marine Corps contracted ESS Technical Support Agency in basic troubleshooting and first echelon maintenance. First echelon maintenance will be defined by Security Division (PS). (Marine Corps Order P5530.14)

7007. SECURITY ENGINEERING. As Chapter 11 (Physical Security) describes, physical security is an important component of AT. ATOs who want to better understand the physical security aspect of AT may pursue certain training courses.

1. Army Corps of Engineers, Learning Center. The U.S. Army Corps of Engineers (USACE) serves the Armed Forces by providing essential engineering services and capabilities. The USACE Learning Center offers a wide range of security engineering and protective design services to help facilities endure terrorist attacks. USACE security engineers are skilled at performing vulnerability analyses and risk assessments to determine the recommended level of protection required for a facility or asset to minimize the impact of a terrorist attack.

The USACE Learning Center offers training classes through their Proponent-Sponsored Engineer Corps Training (PROSPECT) Program. PROSPECT provides both classroom training and distance learning throughout the United States and around the world. Courses can be customized to meet an organization's unique training needs through on-site training that will fit local timeframes. Courses provided by the USACE Learning Center can be accessed through the website at http://pdsc.usace.army.mil/CrsSchedule.aspx.

2. AT Naval Facilities Engineering Command (NAVFAC) Course. The AT NAVFAC Course is offered by the Naval Facilities Engineering Command Engineering Service Center (NAVFAC ESC), Security Engineering Division, Antiterrorism Services Program (ASP). It teaches the fundamentals of antiterrorism through the protection of facilities against terrorist attacks. The course also provides a general overview of best practices and technology-related protection against acts of terrorism. The AT NAVFAC Course further discusses the application of quantitative vulnerability assessments used to assess the vulnerability and

risk associated with the terrorist or criminal targeting of facilities. Registration for and additional information on the NAVFAC Course may be accessed through the website at https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/atfp/atservices_tab:atfp_workshops_tab.

CHAPTER 8

EXERCISES

CHAPTER 8

EXERCISES

8000. GENERAL. While an AT program leverages resources and technology to reduce Marine Corps vulnerabilities, commands will always face some level of risk. If (or when) an attack or incident occurs, commands must be prepared to respond to and recover from the incident. Thus one of the primary responsibilities of an ATO is to develop an annual program that exercises the plan.

An exercise is a simulation of a realistic threat and/or event that requires participants to function in the capacity expected of them in a real-life situation. Its purpose is to enhance operational preparedness by testing policies, plans, procedures, and emergency response personnel. Exercises evaluate current capabilities to determine emergency response disconnects and AT program shortfalls. An ATO should use the lessons learned from an exercise to revise operational plans and guide future exercises.

There are five main exercises that can be conducted: seminars, workshops, tabletops, functional, and full-scale. These exercises are divided into two categories: discussion-based and operations-based. Discussion-based exercises—seminars, workshops, and tabletops—familiarize participants with current plans, policies, agreements, and procedures, or may be used to develop new plans, policies, agreements, and procedures. Operations-based exercises—functional and full-scale—validate plans, policies, agreements, and procedures; clarify roles and responsibilities; and identify resource gaps in an operational environment.

This chapter describes the different types of exercises in the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP, the national standard for all exercises, is a "capabilities- and performance-based exercise program that provides a standardized methodology and terminology for exercise design, development, conduct, evaluation, and improvement planning." This chapter provides the purpose, characteristics, and requirements of each exercise so an ATO has the tools to construct an effective, HSEEP-compliant exercise program. The exercise program that an ATO develops should be comprehensive and progressive. That is, the exercise program should be constructed as a series of increasingly complex exercises in which each successive exercise builds on the previous one until

mastery is achieved. More information on HSEEP can be obtained at https://hseep.dhs.gov/pages/1001_HSEEP7.aspx.

8001. EXERCISE PLANNING. Planning is key to a successful exercise. The planning process for an exercise depends on the type of exercise being conducted. Appendix Q provides Exercise Timelines, a comprehensive roadmap to developing discussion-based or operations-based exercises. It outlines the planning phases, exercise requirements for each phase, exercise materials produced during each phase, and the associated timeline.

1. Exercise Support Team. One of the most important factors of a successful exercise is the creation of a skilled and dedicated support team. The exercise support team is responsible for the foundation, design, development, conduct, and evaluation of an exercise. The support team determines exercise objectives; tailors the scenario to meet exercise goals; and develops documentation used in evaluation, control, and simulation. A successful support team pays attention to detail; organizes their group based on the ICS; employs project management principles; clearly defines roles, responsibilities, and functional area skills; follows a standardized design/development process; and seeks the support of senior officials. The exercise support team should include representatives from the five ICS sections - Command, Operations, Planning, Logistics, and Administration/Finance - and the intelligence section as needed.

a. Command. The Command section is in charge of coordinating all exercise planning activities. The exercise planning team leader heads the Command section and is responsible for assigning exercise activities and responsibilities, providing guidance, establishing timelines, and monitoring the development process. The liasion coordinator and safety controller report to the exercise planning team leader.

b. Operations. The Operations section provides most of the technical or functional expertise for participating entities. This group is responsible for selecting the exercise design objectives and constructing the scenario. Additionally, the Operations section identifies representatives to act as controllers to manage the exercise.

c. Planning. The planning section is responsible for compiling and developing all exercise documentation. To accomplish this effectively, the planning section should collect and review policies, plans, and procedures that will be

validated in the exercise. The planning section is also responsible for exercise evaluation. Functional or full-scale exercises may require the planning section to develop simulated actions for agencies not participating in the exercise.

d. Logistics. The logistics section provides the supplies, materials, facilities, and services necessary to enable the exercise to function smoothly without outside interference or disruption. This group consists of two subsections: service and support. The service section provides transportation, barricading, signs, food and drinks, real-life medical capability, and exercise-site perimeter security. The support section provides communication, purchasing, general supplies, VIP/observer processing, and recruitment/management of victim actors.

e. Administration/Finance. The administration/finance section provides grant management and administrative support throughout exercise development. This section is also responsible for the registration process and for coordinating schedules for the planning team, exercise planning team leader, participating agencies, and the host community or communities.

f. Intelligence Section. A separate intelligence section is often required when the incident requires the collection and dissemination of secured or classified information, such as in the event of a terrorist attack. The intelligence section would be responsible for managing internal information, intelligence, and operational security requirements supporting incident management activities. This may include information security and operational security activities, as well as the complex task of ensuring that sensitive information of all types (e.g., classified information, law enforcement-sensitive information, proprietary information, or export-controlled information) is handled in a way that not only safeguards the information, but also ensures that it gets to those who need access to it to perform their missions effectively and safely.

g. Participants. The exercise planning team size depends on the type of exercise being conducted. Typically, smaller, less complicated exercises, such as seminars and workshops, require a core group of four or five people. Larger, more complicated exercises require additional team members. Planning team members' involvement in the exercise process makes them ideal selections for exercise facilitator, controller, and/or evaluator positions. However, it is recommended that planning team members do not serve as players in the exercise.

8002. SEMINARS. Although ATOs should fully understand emergency response plans, policies, and procedures, other Marine Corps personnel may not be as familiar with their duties and responsibilities. Orientation seminars are discussion-based exercises that provide an ATO with the opportunity to train and familiarize personnel with policy, responsibilities, and tasks in the emergency management system. An orientation seminar is characterized by low stress, little attention to real time, and a lower level of preparatory effort. Seminars are basic, informal exercises that do not involve simulation. They are designed to elicit constructive discussion by participants as they examine the jurisdiction's emergency management policy, then resolve problems based on existing emergency operations plans. Seminars provide a valuable means to test new or experimental plans and to orient new staff members or leaders.

1. Participants. Seminars should involve all agencies that have an emergency management function related to the exercise. Each function/service should have one or two representatives at a seminar. These representatives should be involved in management, policy, coordination, and/or operations. A facilitator leads a seminar.

8003. WORKSHOPS. Workshops are discussion-based exercises similar to seminars, but different in two important aspects: participant interaction is increased and the focus is on achieving or building a product (plans and policies). Workshops provide a highly interactive and collaborative setting in which participants identify, exchange, plan, and elaborate on emerging ideas, high-quality research, and/or cutting-edge practices. Seminar participants examine overall emergency response plans and procedures, but effective workshops must focus on a specific issue and a clearly defined goal. Typically, workshops begin with a presentation or briefing that explains the rationale for the workshop and the specific tasks and expected outcomes of the exercise. Workshop goals may include identifying issues that may arise when developing a coordinated response plan, defining new regional response plans, determining program or plan objectives, developing an exercise scenario, and/or determining evaluation elements or performance standards.

1. Participants. Workshops should involve all agencies that have an emergency management function related to the exercise. Similar to a seminar, each function/service should have one or two representatives at a workshop. These representatives should

be involved in management, policy, coordination, and/or operations. A facilitator leads a seminar, but should assume a less direct role and encourage more participation in a workshop.

8004. TABLETOP EXERCISES (TTXs). TTXs are discussion-based exercises that analyze an emergency situation in an informal environment without the time pressures of an actual simulation of events. TTX participants discuss general problems and procedures in the context of an emergency scenario. A TTX is conducted to discover any deficiencies in established plans and procedures, and to discuss plausible solutions if the particular scenario were to occur. It typically begins with a narrative describing the event and problems confronting emergency responders. Participants then brainstorm ways to solve the issues presented. At certain times during the discussion, injects that alter the intensity of the situation in the simulation and advance the discussion will be presented.

TTXs have several advantages and disadvantages. The advantages are that it is removed from the planning team; it requires only a modest commitment in terms of time, cost, and resources; it is an effective method of reviewing plans, procedures, and policies; and it is a useful way to acquaint key personnel with emergency responsibilities, procedures, and each other. The disadvantages are that it is not as realistic as an operations-based exercise; it provides a limited exercise of plans, procedures, and staff capabilities; and it does not provide a practical way to demonstrate system overload.

1. Participants. All agencies that have an emergency management role should actively participate in a TTX. Each function/service should have one or two representatives at the exercise. These representatives should be policy, coordination, and/or operations managers. A TTX is led by a facilitator who presents the narrative and scenarios and guides the discussion.

8005. FUNCTIONAL EXERCISES (FEs). FEs are operations-based exercises that simulate an emergency in the most realistic manner possible, short of moving real people and equipment to an actual site. Its purpose is to test or evaluate the capability of one or more functions in the context of an emergency. An FE is an interactive exercise designed to challenge the entire emergency management system. It tests the same functions and responses that would be tested in a full-scale exercise (FSE), without the high costs or safety risks of moving personnel and equipment. An FE usually takes place at an EOC or other

operations center that would be the central location designated in a real emergency for policy decisions, coordination, control, and overall planning.

FEs are well suited to assess the performance of emergency responders; the management of an EOC, command posts, headquarters, and staff; the effectiveness of established policies and procedures; the adequacy, appropriation, and acquisition of resources; interjurisdictional relationships; and the communication system.

An FE is a complex exercise that requires the creation of injects, a master scenario events list (MSEL), and a simulation cell (SIMCELL). Injects are instructions for an exercise controller that detail the proper way to interact with players while relaying specific, detailed, and time-critical information intended to elicit a specific, measurable response from one or more players. Injects are delivered via any communication tool that is to be evaluated during the exercise. A MSEL is a compiled list of all expected player activities, planned controller activities (injects), and any exercise notes. A SIMCELL is staffed by exercise managers and SIMCELL controllers, and delivers injects to the controller and players. Multiple phone lines, fax machines, radios, and a copier are all required for SIMCELL operation.

1. Participants. FE participants include a controller, players, simulators, and evaluators. The controller supervises the simulation and overall conduct of the exercise, ensuring that the exercise proceeds as planned and that objectives are reached. The players in an FE are those who hold key decision-making or coordinating positions and would typically work in the operations center. The role of the players is to respond to the scenario as they would in a real emergency. Simulators portray the organization that would normally interact with those in the operations center by delivering messages—descriptions of events or problems—that require players to act. Evaluators observe the actions and decisions of the players so that they can report successful actions and areas for improvement. To effectively evaluate an FE, evaluators must be familiar with the objectives, exercise scenario, and the jurisdiction or organization that is undertaking the exercise.

8006. FULL-SCALE EXERCISES. FSEs are operations-based exercises that combine the interactivity of an FE with a field element. It tests the existing plans and methods of an organization by

creating realistic situations that require the mobilization and use of actual equipment, personnel, and resources. An FSE is as realistic as possible. It is a lengthy and resource-intensive exercise that takes place in the field and uses the personnel and equipment that would be needed in a real event. It tests the coordination of policy and management officials with field forces. An FSE should draw on knowledge of policies, plans, and procedures gained from previously conducted exercises. It should include an activated EOC, exercise most functions, and coordinate the efforts of several agencies. FSEs involve one or more controllers, the participants, the simulators, the evaluators, and a safety officer. As in an FE, the controller is responsible for supervising the exercise.

1. Participants. FSE participants should include policymakers, coordination personnel, operations personnel, and field personnel. Simulators and evalutors conduct the same duties as in an FE. A safety officer analyzes the entire exercise to ensure there are no safety issues during the exercise. FSEs require a significant investment of time, effort, and resources. It typically takes 1 to 1½ years to develop a complete exercise package.

8007. AFTER-ACTION REPORTS (AARs). AARs are a crucial element to the development and improvement of AT policy, plans, and procedures. The evaluation team, which may include members of the planning team, compiles AARs to analyze the achievement of the intended goals for the exercise. An AAR documents areas of effectiveness and areas for improvement in relation to the exercise objectives. It should include recommendations to solve the problems encountered during the exercise. An AAR should be specific and comprehensive, but its length will vary depending on the size and scope of the exercise.

1. Marine Corps Center for Lessons Learned (MCCLL). In accordance with with MCO 3504.1, all Marine Corps commands and activities must submit AARs to the MCCLL for all major exercises. Disseminating AARs is important for two reasons: (1) dissemination allows other Marine Corps entities to benefit from these operational experiences, and (2) AARs can be used by advocates and proponents to support important changes to the Marine Corps AT program. AARs may be submitted electronically via the MCCLL Web site at http://www.mccll.usmc.mil for unclassified information, or at http://www.mccll.usmc.smil.mil for classified information.

2. Improvement Plan (IP). Based on the AAR, an ATO should develop an IP that implements the recommendations made in the AAR. Crafting AARs/IPs requires the same attention to detail that a planning team must employ for the successful completion of an exercise. An ATO should use previous AARs and IPs as guides in the development of a comprehensive and progressive exercise program.

CHAPTER 9

RESOURCE APPLICATION AND FUNDING

CHAPTER 9

RESOURCE APPLICATION AND FUNDING

9000. GENERAL. In order for an AT program to successfully protect the assets and mission of the Marine Corps, resources must be available to execute an AT plan. Generating resource requirements and acquiring additional resources to mitigate identified vulnerabilities is a key step in reducing risk. As installation and unit personnel make plans for any operation, competing requirements stress finite resources. The limited availability of resources puts a premium on proper planning and justification of resources. A realistic and affordable fiscal year (FY) budget and procurement strategy should be developed that captures total life-cycle costs (staffing needs, training costs, logistics/maintenance, and replacement costs). However, before installations or units can compete for and acquire resources, AT requirements must be well-defined, formally documented, and prioritized. The FY budget and procurement strategy should hinge on the prioritized list of risks generated from the risk management process detailed in Chapter 3. The prioritized list of risks is intended to help ATOs identify AT program needs so that funding can effectively address the most serious shortcomings. Once AT requirements are documented and prioritized, the ATO and the Financial Manager (FM)/Comptroller should work together to formulate a budget to address AT requirements. Several funding avenues, each described in this chapter, should be considered when developing budget and AT funding requests.

9001. DETERMINING RESOURCE REQUIREMENTS. Once an AT plan is developed, an ATO assists in determining the resource requirements needed to execute the AT plan. Generally resource requirements include staffing, operations, training, exercises, equipment, C4 and ESS systems, and physical security requirements for barriers, access control points, and facilities. In determining the necessary level of resource requirements, an ATO and the ATWG, in conjunction with CIP, CBRNE, Emergency Management, the PMO, and, when appropriate, the EOD and Fire Chief, should analyze the overall list of prioritized risks produced during the risk management process. After all risks have been analyzed and the AT plan has been developed, an ATO should have a clear understanding of the resource requirements needed to execute the plan. The ATO should consider all tactics, techniques, and procedures that may mitigate risks while understanding that the cost of mitigation